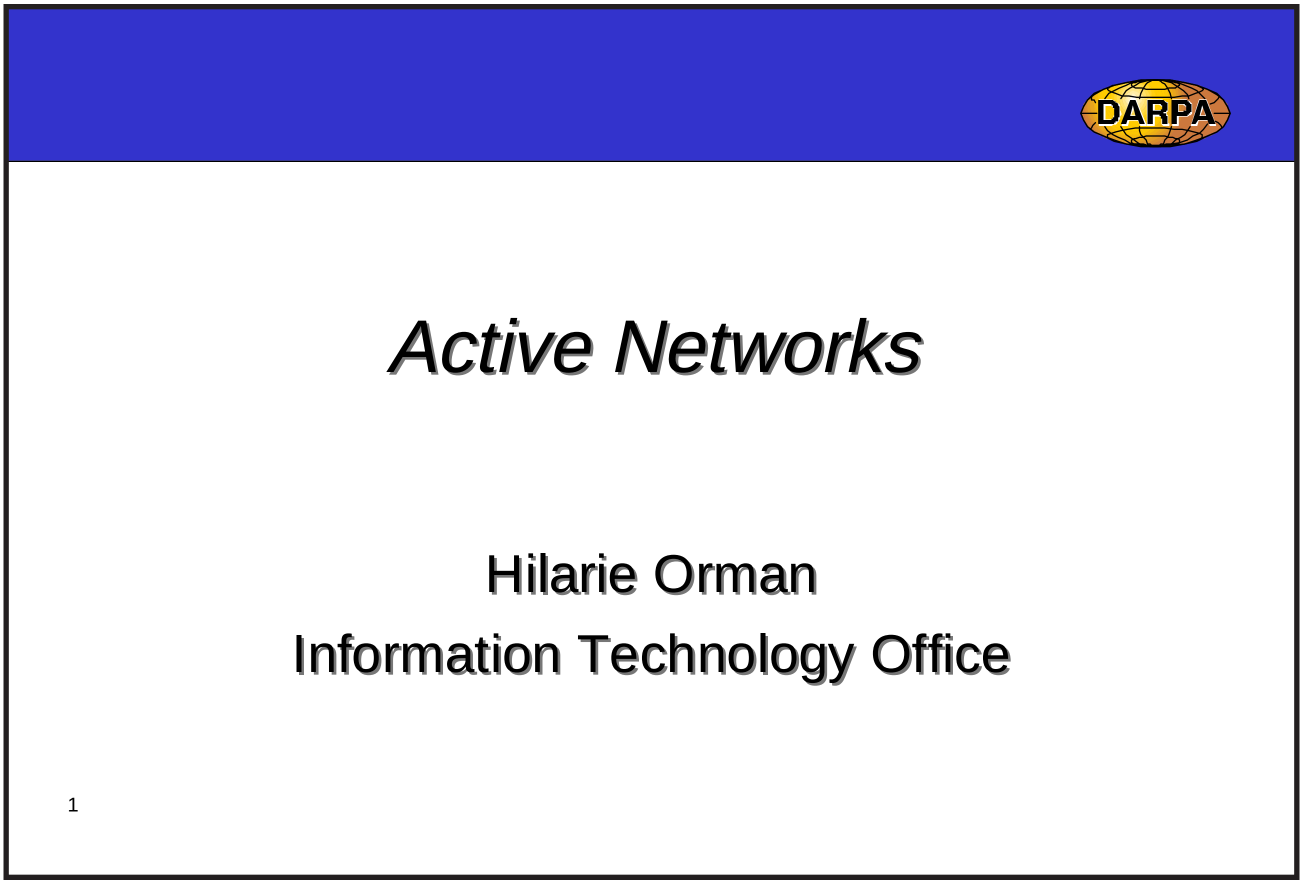
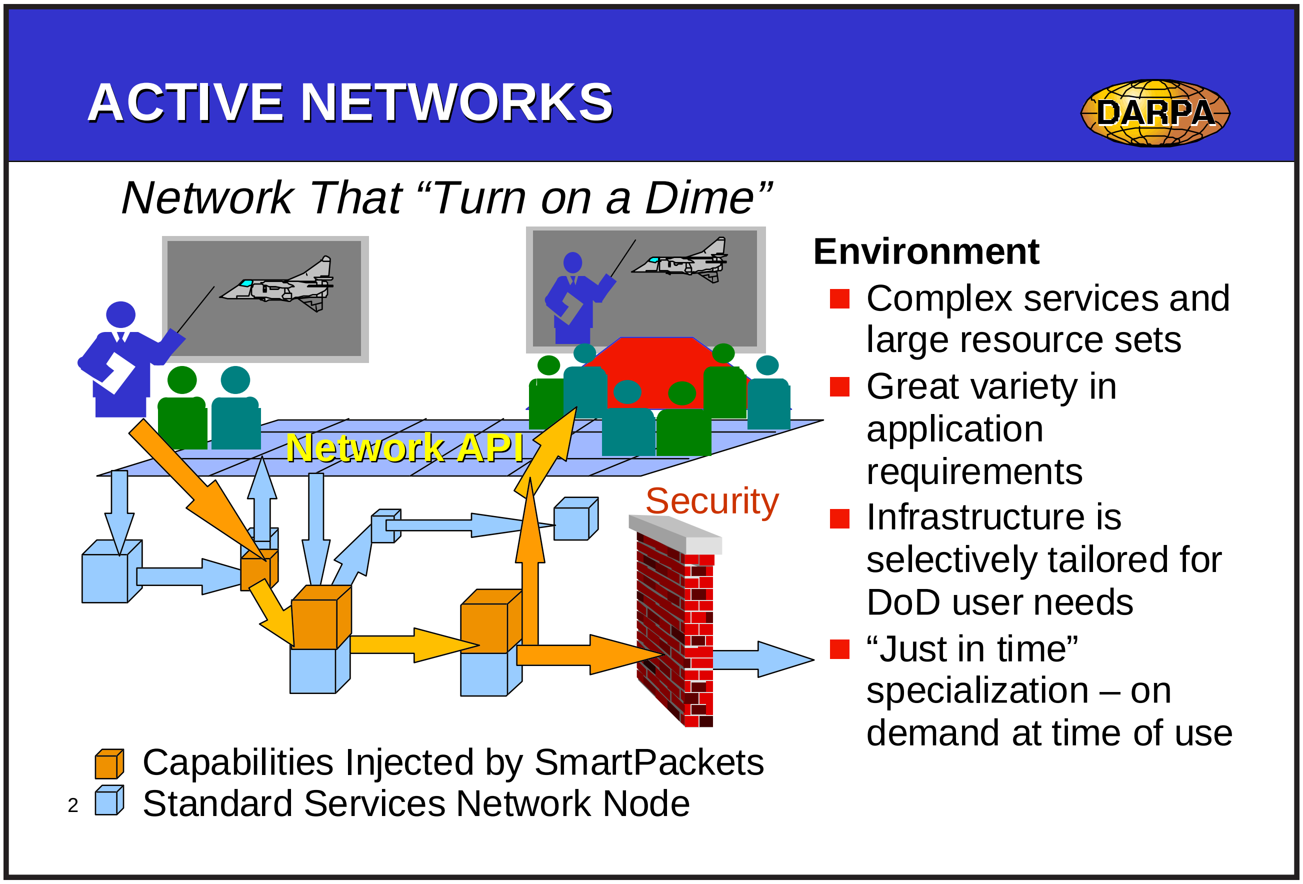


Active Networks

Hilarie Orman

Information Technology Office



ACTIVE NETWORKS

DARPA

Network That "Turn on a Dime"

Environment

- Complex services and large resource sets
- Great variety in application requirements
- Infrastructure is selectively tailored for DoD user needs
- "Just in time" specialization – on demand at time of use

🟧 Capabilities Injected by SmartPackets

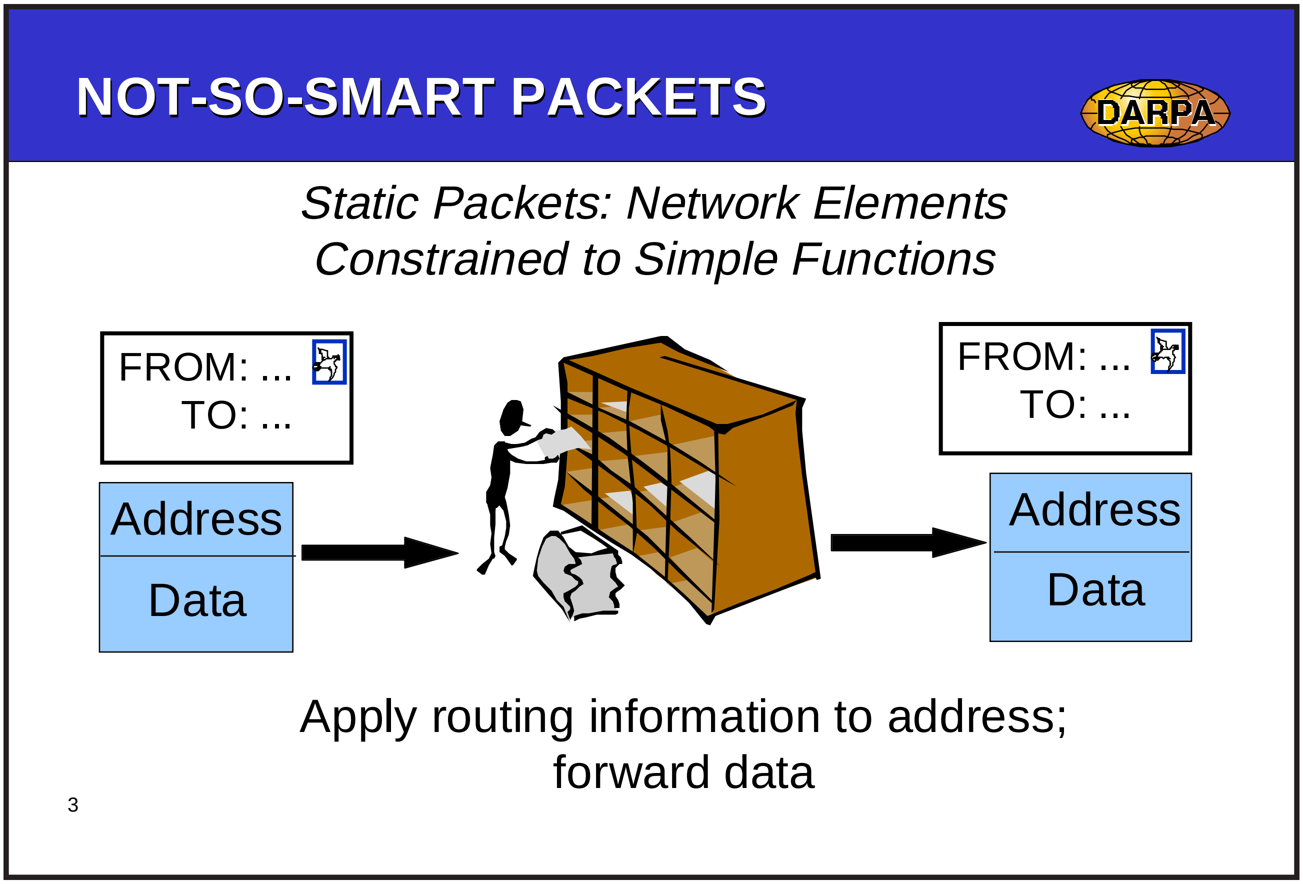
2 🟦 Standard Services Network Node

Active networking is a revolutionary networking technology, bringing specialized communication processing into the network fabric itself. DoD networking needs are highly demanding in several dimensions of service, and this mandates specialization of service during real-time operation, even when the connections span heterogeneous networking technologies. Active networking technology can bring specialized services to the exact points in the networking fabric where leverage is greatest. This balances communications processing between the network and the end systems.

The current strategy of defining a standard networking software base for the interior network nodes results in a rigid system that changes slowly over time; active networks shatter the paradigm. The agility of active networking makes it unnecessary to achieve consensus on global standards for basic data transfer because data processing algorithms move within the network with the same ease as does data.

New capabilities:

- Just-in-Time Delivery of Communication Services to Places of Use
- Tailor Communication Services Directly to the User Needs
- Superior Data Communication Services
- Balance Communications Processing Between the Network and the Applications
- Break the Global Standardization Paradigm
- Enable New DoD Applications in Partnership With Industry Practices



NOT-SO-SMART PACKETS

Static Packets: Network Elements Constrained to Simple Functions

FROM: ...
TO: ...

Address

Data

FROM: ...
TO: ...

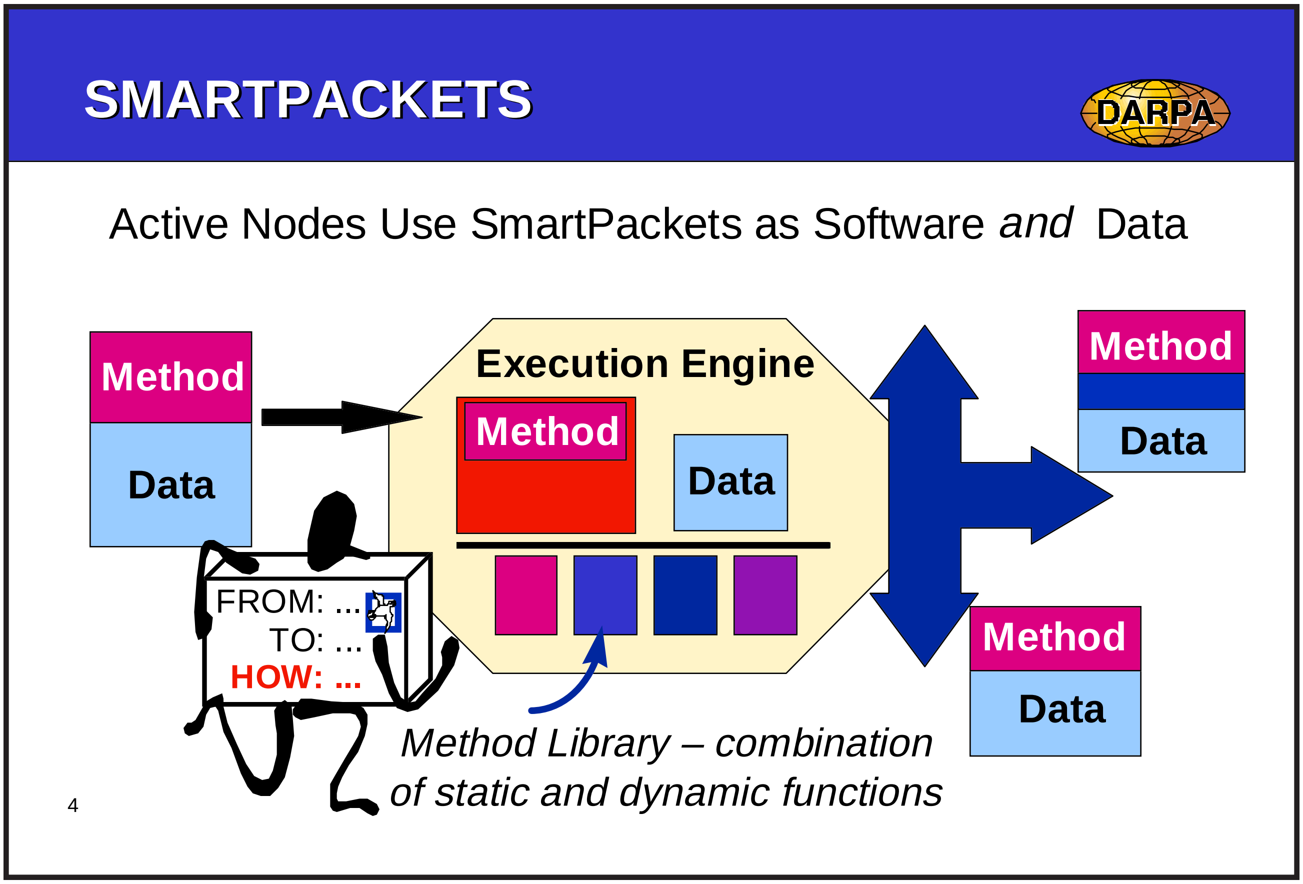
Address

Data

Apply routing information to address; forward data

3

Today’s packets are static and similar to ordinary postal letters. They are subject to a single processing paradigm within the network: routing toward their destination is based on information in the packet header. Network elements maintain only enough state to ensure connectivity.



SMARTPACKETS

DARPA

Active Nodes Use SmartPackets as Software *and* Data

Method

Data

Execution Engine

Method

Data

FROM: ...
TO: ...
HOW: ...

Method

Data

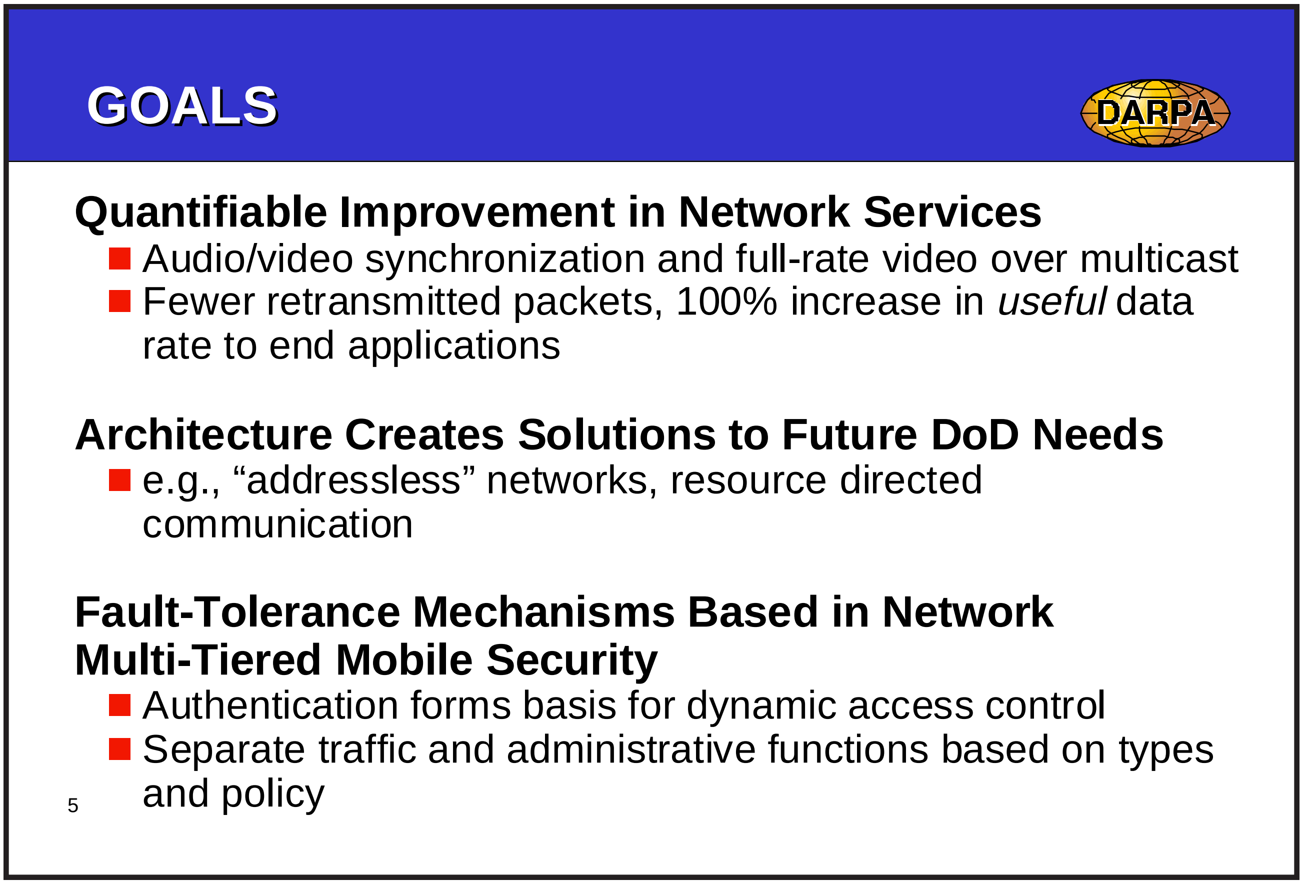
Method

Data

Method Library – combination of static and dynamic functions

Active Network data transfer is based on SmartPackets. SmartPackets include program methods, or “how-to” information, in addition to data and addressing. These methods turn the network elements into active elements: they apply the methods to the packets, thereby implementing network-based services tailored to the application. The active part of a packet can travel with the data, be copied from node to node, be resident in the node permanently or temporarily. The library of methods opens up the traditional networking system to composable, mix-and-match services that tailor the handling to special packet requirements.

Special services can be built with relatively simple primitives: copy, split, join, trace, and count. The primitives combine to replace and extend traditional networking services: echo, trace, flood, etc.



GOALS

Quantifiable Improvement in Network Services

- Audio/video synchronization and full-rate video over multicast
- Fewer retransmitted packets, 100% increase in *useful* data rate to end applications

Architecture Creates Solutions to Future DoD Needs

- e.g., “addressless” networks, resource directed communication

Fault-Tolerance Mechanisms Based in Network

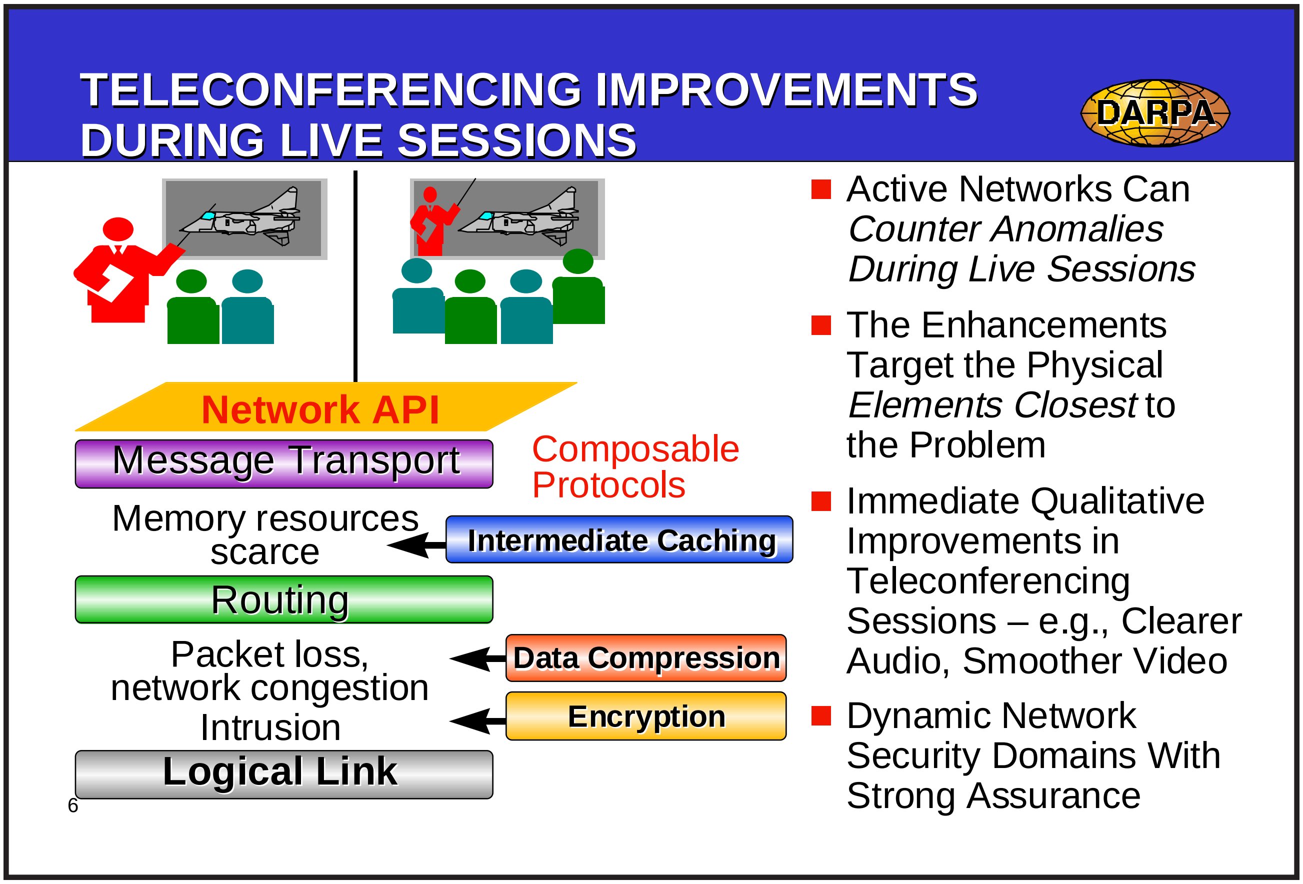
Multi-Tiered Mobile Security

- Authentication forms basis for dynamic access control
- Separate traffic and administrative functions based on types and policy

The goal of the Active Networks program is to develop and test a protocol architecture that allows rapid and dependable creation, reconfiguration, and deployment of new networking services. The Active Network achieves this goal through the concept of SmartPackets, self-directed data units, which can direct their own processing and deliver new services to the interior network nodes. The program is focused on the technology for processing SmartPackets securely and on building enhanced services from generic network software elements. The result will be networks with greatly improved communication services that meet user requirements efficiently and securely.

Success will be demonstrated by solving a series of challenge problems by using new network addressing mechanisms and by injecting new multimedia services that reduce data loss during live video teleconferences on the Internet. Some of the new service elements will affect the entire network; others will be used only where needed. Improvements will be both measurable and readily evident in the resulting systems (e.g., improved image quality, better voice synchronization, fewer failures, or faster recovery from failures).

Throughout the execution of the program, projects addressing the security and stability of Active Networks will maintain a first-class presence in visibility and influence, making the new technology suitable for quick incorporation into DoD networks.



TELECONFERENCING IMPROVEMENTS DURING LIVE SESSIONS

DARPA

Network API

Message Transport

Composable Protocols

Memory resources scarce

Intermediate Caching

Routing

Packet loss, network congestion

Data Compression

Intrusion

Encryption

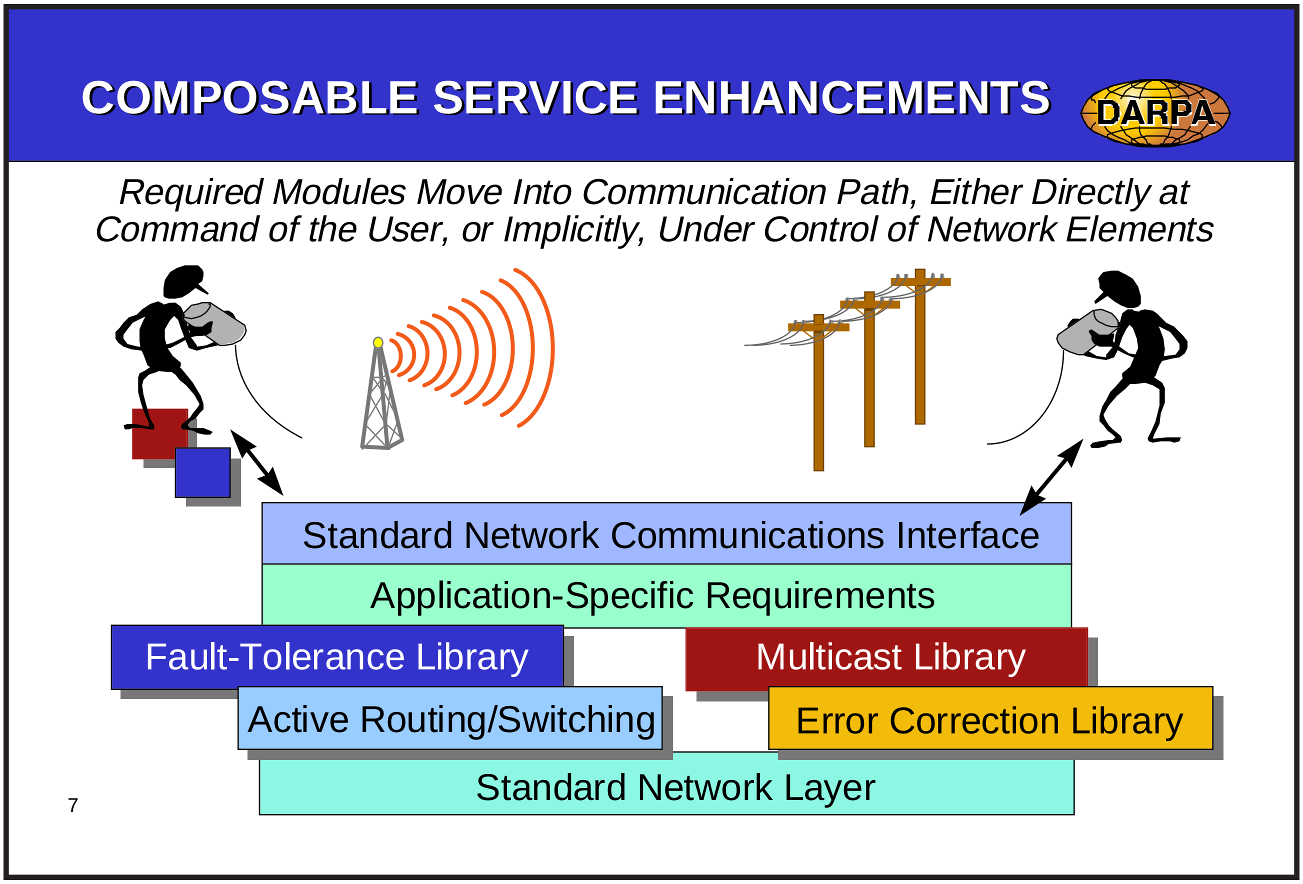
Logical Link

- Active Networks Can *Counter Anomalies During Live Sessions*
- The Enhancements Target the Physical *Elements Closest* to the Problem
- Immediate Qualitative Improvements in Teleconferencing Sessions – e.g., Clearer Audio, Smoother Video
- Dynamic Network Security Domains With Strong Assurance

6

Group teleconferencing is an emerging application that illustrates the need for active technology, due to the complex and dynamic nature of the communication. No single strategy will deliver high-quality results to all sites all the time, but active technology allows sites to dynamically compose in-the-network solutions to their communications needs. Services, such as data compression, encryption, and caching, can slide in and out of the network paths on a link-by-link basis, balancing capacity, cost, and error rates against end-to-end requirements.

Active elements will have the ability to enforce security policies for properly authenticated data elements and principals. This constitutes a flexible and novel basis for cooperative, dynamic security domain establishment.



COMPOSABLE SERVICE ENHANCEMENTS

DARPA

Required Modules Move Into Communication Path, Either Directly at Command of the User, or Implicitly, Under Control of Network Elements

Standard Network Communications Interface

Application-Specific Requirements

Fault-Tolerance Library

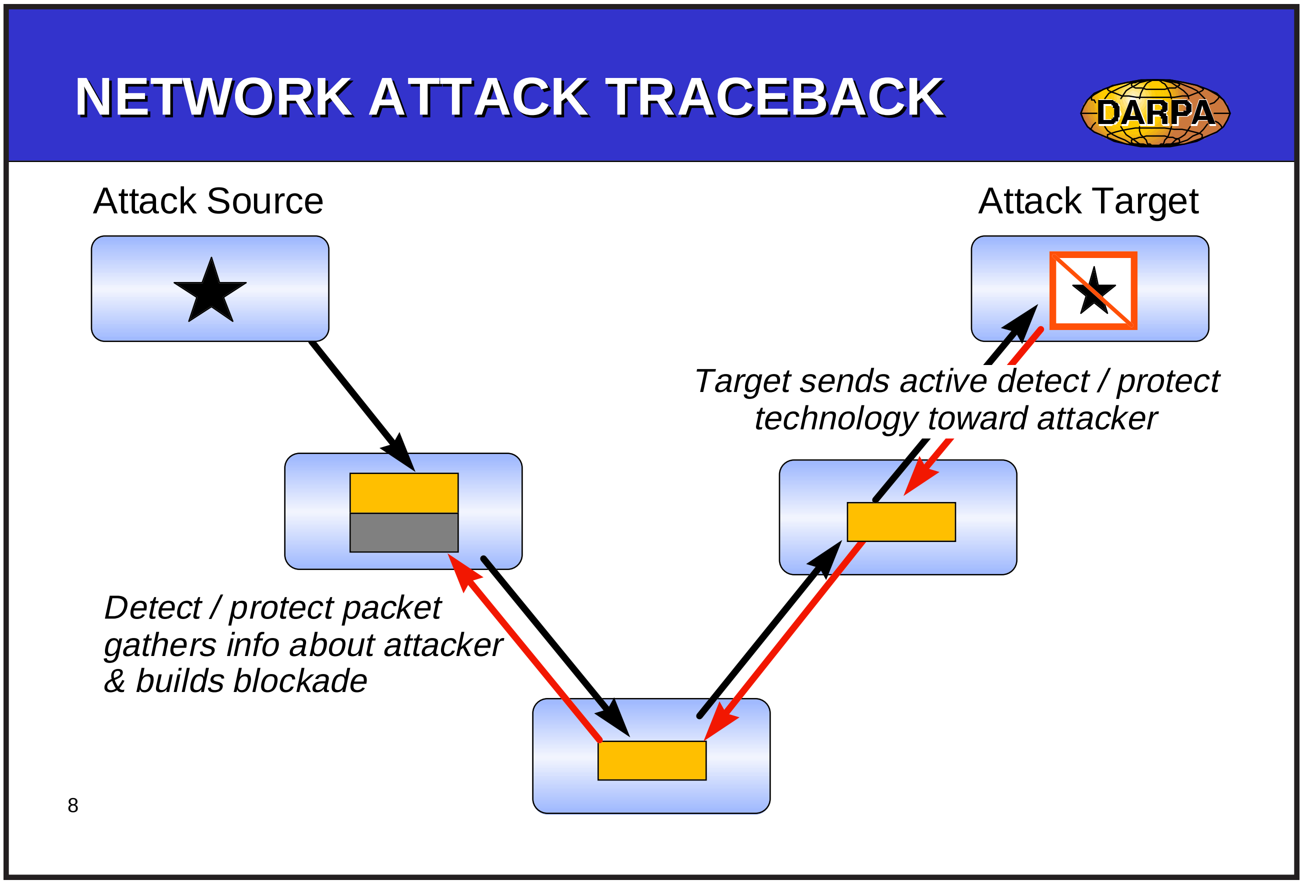
Multicast Library

Active Routing/Switching

Error Correction Library

Standard Network Layer

There are many opportunities for end-users to make use of active networks in heterogeneous networking situations, where data span several technologies, but must still meet overall requirements. Services can slide in and out of the network protocol stack, achieving specialization quickly.



NETWORK ATTACK TRACEBACK

DARPA

Attack Source

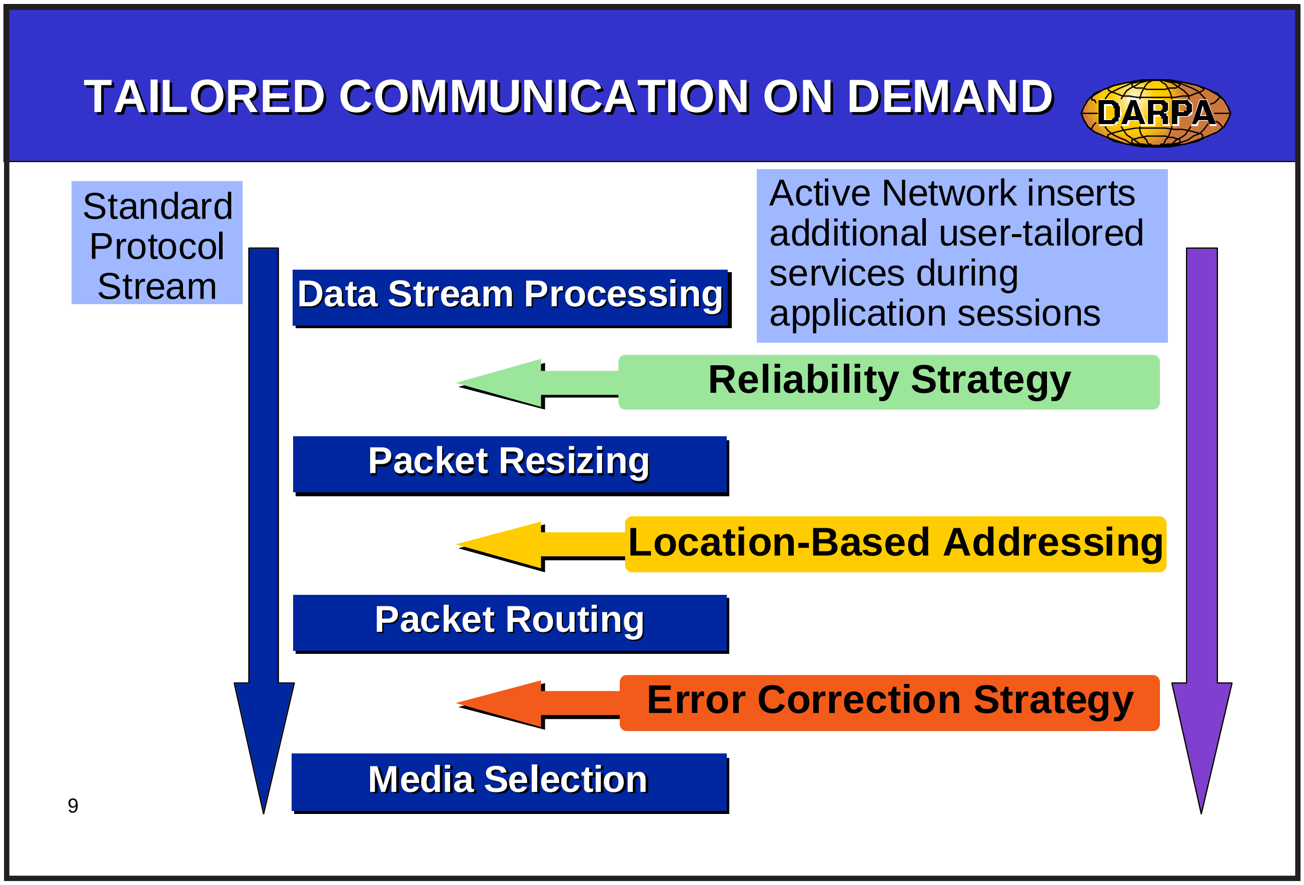
Attack Target

Target sends active detect / protect technology toward attacker

Detect / protect packet gathers info about attacker & builds blockade

8

Active networking technology can build new networking structure for survivability, on a dynamic basis. In a scenario that has been demonstrated in prototypes, active networking technology can deliver defensive solutions in response to recognized network attacks. A difficult problem for system administrators is to quickly identify the sources of attacks in order to stop the attack close to its source. Active networks can deliver "traceback" capability, inverting the routing path selectively and delivering preventative technology to the *uncompromised* sites nearest to the attack. The solution software is "safe" with respect to networking policies because it only affects packets intended for the victim's site, no others. This illustrates the need for security technology and high-assurance systems within the active network.



TAILORED COMMUNICATION ON DEMAND

DARPA

Standard Protocol Stream

Active Network inserts additional user-tailored services during application sessions

Data Stream Processing

Reliability Strategy

Packet Resizing

Location-Based Addressing

Packet Routing

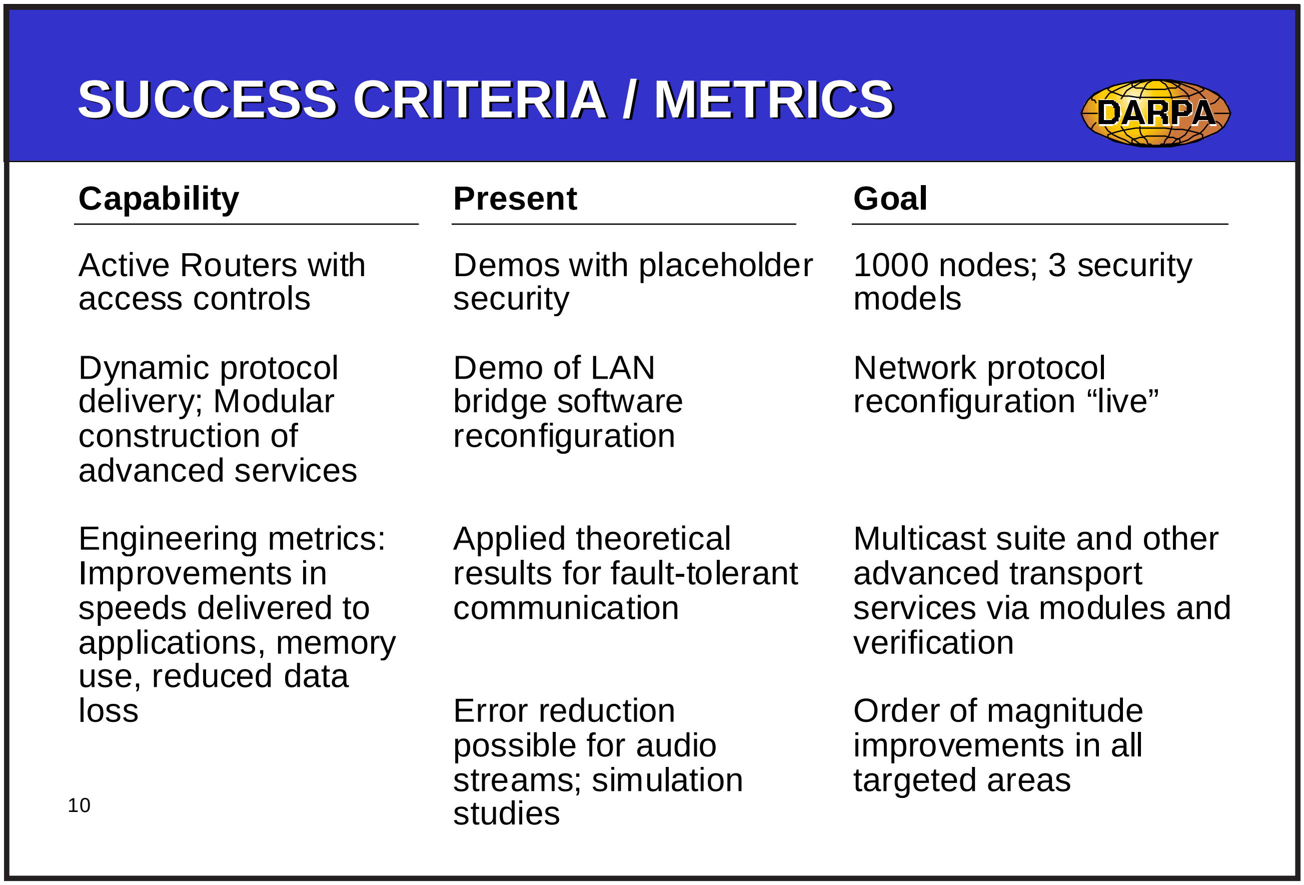
Error Correction Strategy

Media Selection

9

The most exciting aspect of active technology is the promise of extending networks to radically different ways of moving data. Standard protocol stacks deliberately limit their effect on data units to small, simple operations, even when extra processing power is available. Today’s networks also rely exclusively on names and addresses for matching data to destination. Active networks can move beyond this, integrating distributed processing techniques into the network fabric, achieving efficiencies by eliminating roundtrips, automating load balancing, and achieving data replication and locality through in-the-network service architectures.

The sophistication of tailoring can naturally extend through the network protocol stack, automatically making trade-off decisions that may result in acquiring specialized software solutions to intermittent or highly anomalous behavior; sophisticated data coding is an example of a technique that would probably ameliorate many networking problems today, but it is not widely deployed because of the difficulty of integrating the software into end systems.



SUCCESS CRITERIA / METRICS

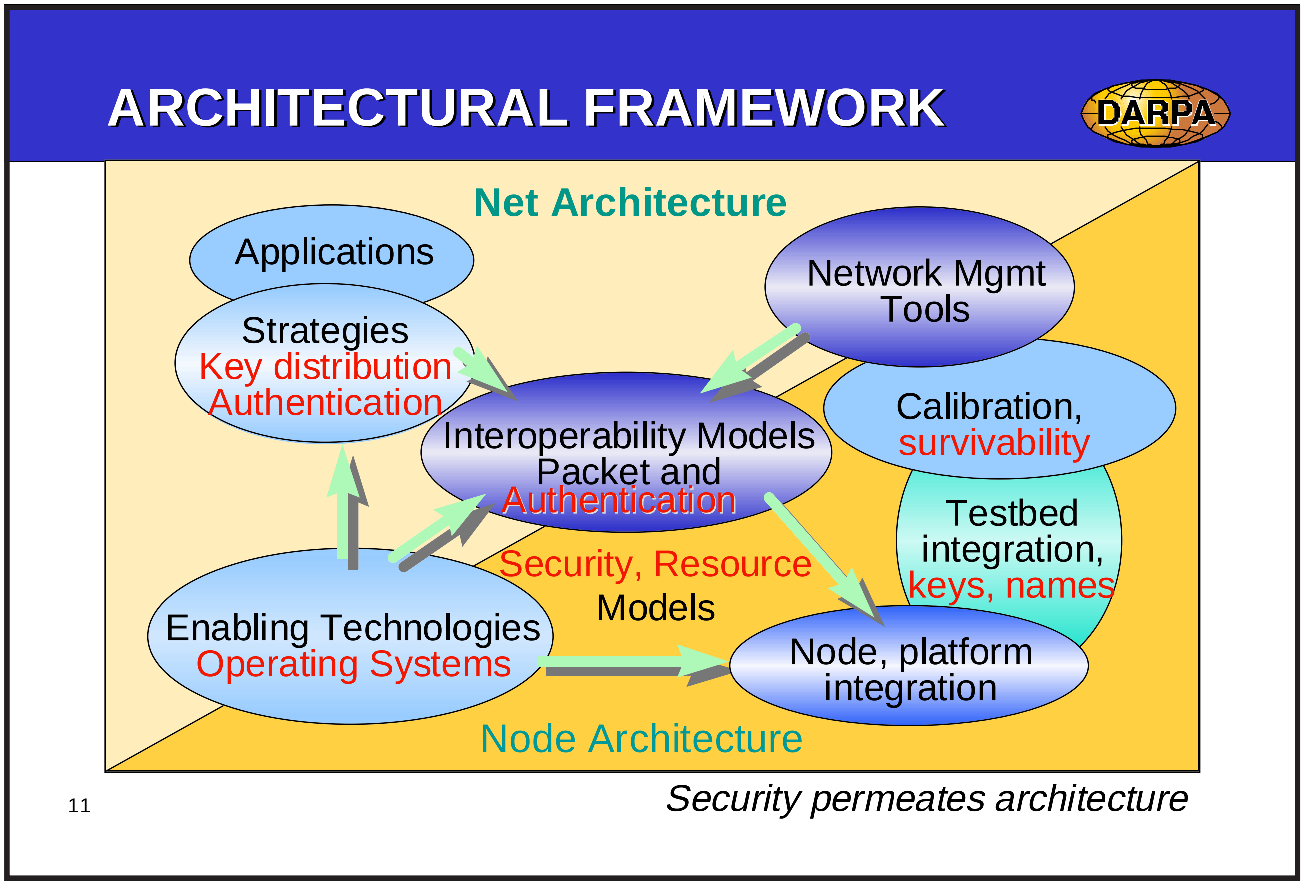
DARPA

Capability	Present	Goal
Active Routers with access controls	Demos with placeholder security	1000 nodes; 3 security models
Dynamic protocol delivery; Modular construction of advanced services	Demo of LAN bridge software reconfiguration	Network protocol reconfiguration "live"
Engineering metrics: Improvements in speeds delivered to applications, memory use, reduced data loss	Applied theoretical results for fault-tolerant communication	Multicast suite and other advanced transport services via modules and verification
	Error reduction possible for audio streams; simulation studies	Order of magnitude improvements in all targeted areas

10

Success criteria for the program are based on measurable improvements over today's advanced services. We expect researchers to develop and distribute improvements in teleconferencing techniques to each other, for example, running bake-off tests throughout the program lifetime. As new architectural frameworks for specialized services become available, they can be adopted quickly by the testbed sites.

An initial interoperation capability was developed over the summer. We will be expanding the number of organizations, and the existing organizations will be increasing the sophistication of their implementations as new services are developed.



ARCHITECTURAL FRAMEWORK

DARPA

Net Architecture

Applications

Strategies
Key distribution
Authentication

Network Mgmt
Tools

Interoperability Models
Packet and
Authentication

Calibration,
survivability

Testbed
integration,
keys, names

Security, Resource
Models

Enabling Technologies
Operating Systems

Node, platform
integration

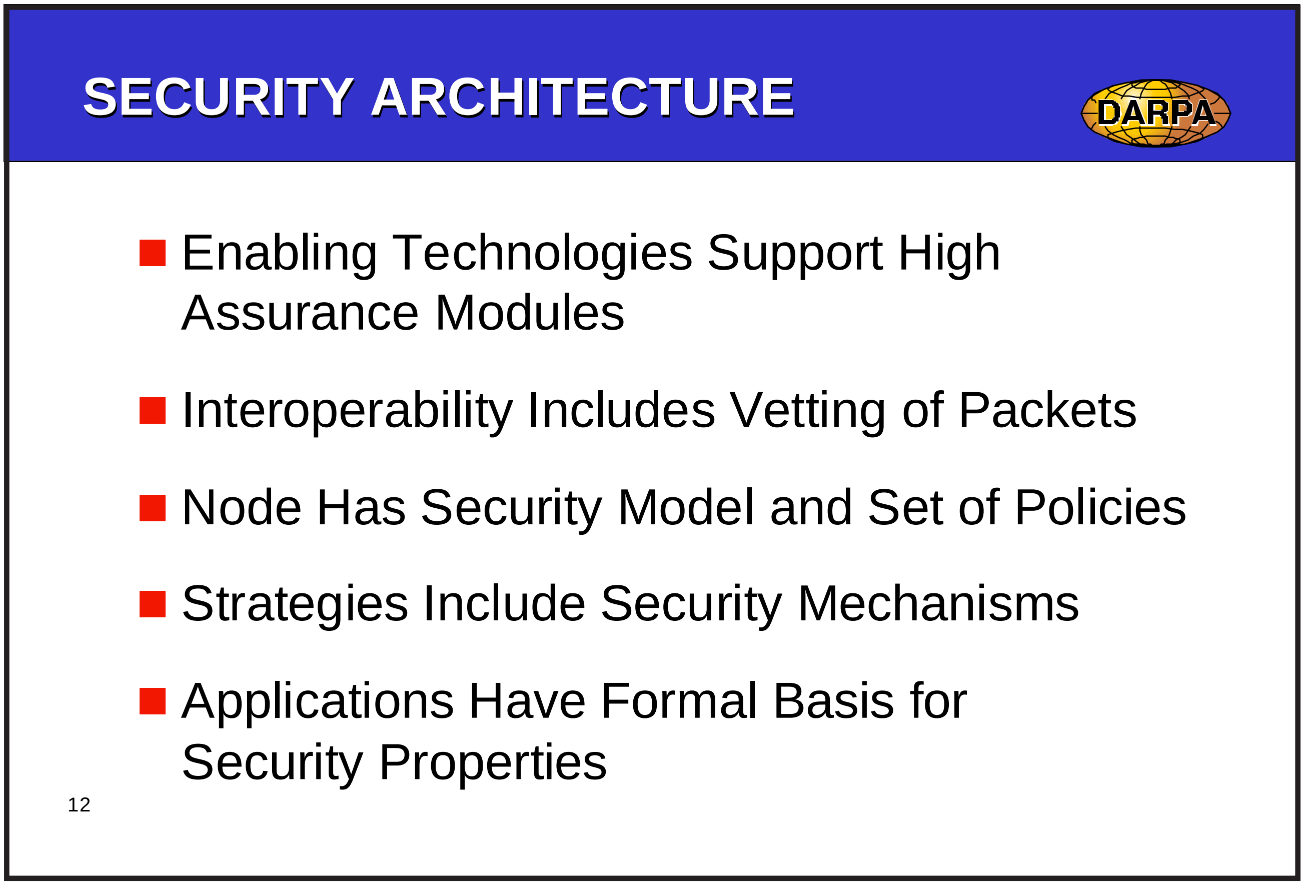
Node Architecture

11

Security permeates architecture

The technological components comprising the active network architecture are illustrated here, emphasizing the "pressure points" for security underpinnings. The architecture is depicted showing the elements that define the network nodes and those that, taken together, form the network service model.

Security of design and mechanism is essential for active networks – a general computation capability cannot be universally supported without a framework for resource control, correct handling of data, and strong guarantees of authentication and correct operation.



SECURITY ARCHITECTURE

- Enabling Technologies Support High Assurance Modules
- Interoperability Includes Vetting of Packets
- Node Has Security Model and Set of Policies
- Strategies Include Security Mechanisms
- Applications Have Formal Basis for Security Properties

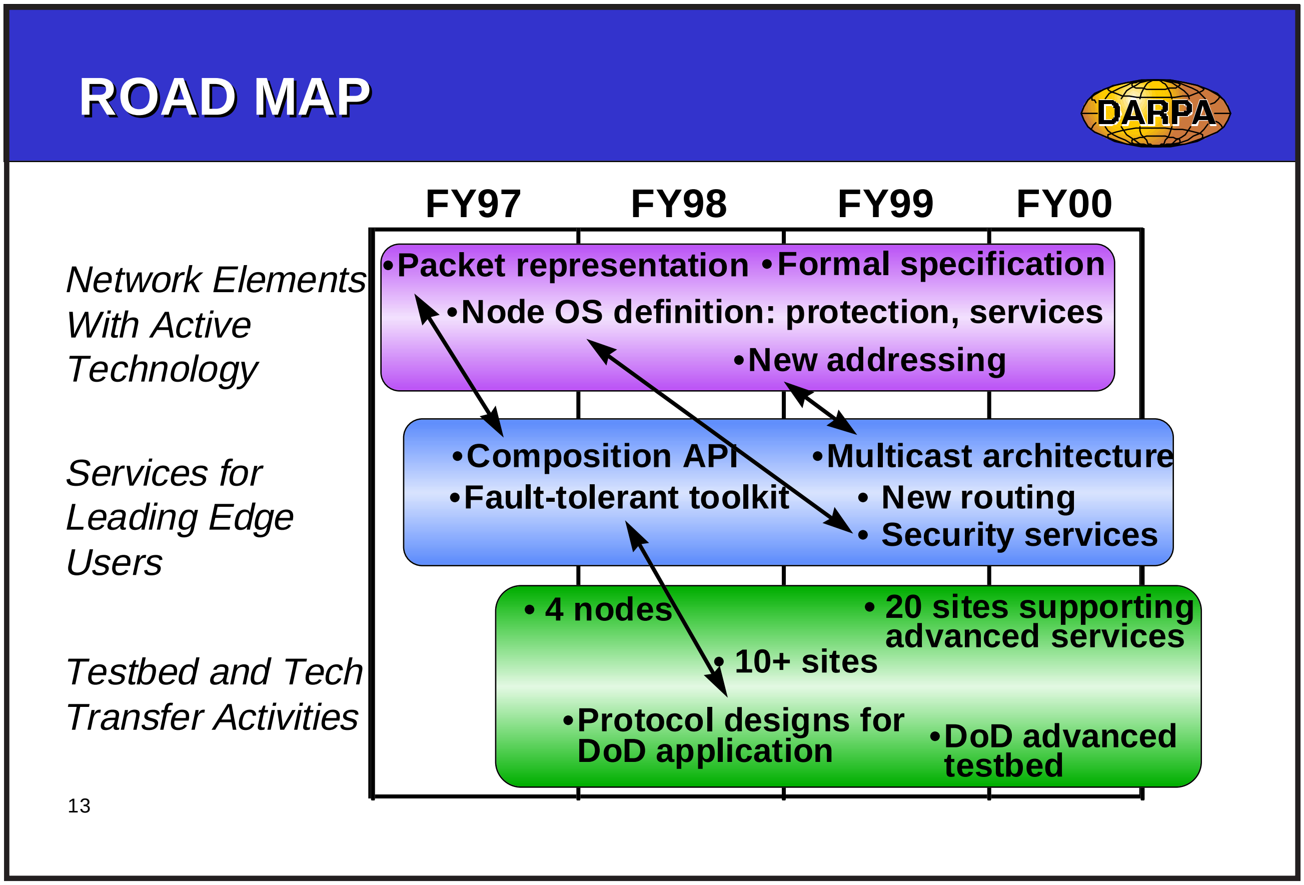
The security architecture is multi-purpose, supporting inter-organizational network access and routing policies, high-assurance in-the-network applications, end user needs, and the integrity of the active network itself.

The basic policy requires multi-part provenance and integrity checking for address (if present), methods, and data. This forms the basis for access control.

Each node has a set of resources that it protects, and nodes cooperate to form consistent resource allocations for data flows. Resources include CPU cycles, permanent and temporary storage, bandwidth, routing tables, etc.

The basic security model treats each data flow as a separate “principal,” and to first order, there is no interference between flows. There will be a spectrum of intermediate models, each authorizing more sharing or more privilege.

High levels of privilege will be required for modifying basic resources, such as kernel memory, audit and monitoring functions, and installing protocols that affect the ability to load new protocols.



ROAD MAP

FY97 FY98 FY99 FY00

Network Elements With Active Technology

- •Packet representation
- •Formal specification
- •Node OS definition: protection, services
- •New addressing

Services for Leading Edge Users

- •Composition API
- •Fault-tolerant toolkit
- •Multicast architecture
- • New routing
- • Security services

Testbed and Tech Transfer Activities

- • 4 nodes
- • 10+ sites
- • 20 sites supporting advanced services
- •Protocol designs for DoD application
- •DoD advanced testbed

13

The roadmap shows three main tracks: the network elements, the services, and the testbed/tech transfer activities. These are focused on the goal of transition to enhanced networking services for DoD advanced users on high speed networks.

The Active Network concept will change the deployment strategy for network software, enabling specialized tailoring of network resources with greatly reduced costs in the areas of staff time and configuration control, and increased speed of propagation of the software changes. This concept of rapid, easy deployment may be the only viable approach for making major improvements to today’s internet technology and assuring information dominance throughout the next century.